

JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Sheueling Chang Shantz et al.

Title: METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR
INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY
CRYPTOGRAPHY

Application No.: 10/626,420 Filed: July 24, 2003

Examiner: Sheikh, Ayaz R. Group Art Unit: 2131

Atty. Docket No.: 004-9388 Confirmation No.: 9856

December 7, 2004

Mail Stop Amendment
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450**INFORMATION DISCLOSURE STATEMENT**
37 C.F.R. § 1.97(b)

Dear Sir:

Pursuant to 37 C.F.R. § 1.56, § 1.97 and § 1.98, the undersigned brings to the Examiner's attention in the above-identified application the patents, publications, applications or other information identified in the attached:

- Form(s) PTO/SB/08A (1 page(s), with copy of 1 reference(s)).
- Form(s) PTO/SB/08B (1 page(s), with copy of 3 reference(s)).
- Listing of Pending Applications (N/A page(s), with copy of no application(s)).
- Other: N/A

Citation of such information shall not be construed as (i) an admission that the information necessarily is, or corresponds to, prior art with respect to the instant invention, (ii) a representation that a search has been made, other than as described herein, or (iii) an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

For each item of information listed that is not in the English language, the undersigned has provided a concise explanation of the relevance through (i) an English language abstract, (ii) an English language equivalent application, or (iii) if cited in a search report or other action by a foreign patent office in a counterpart foreign application, an English language version of the search report or action that indicates the degree of relevance found by the foreign office.

CERTAIN COPIES NOT INCLUDED

Pursuant to operative regulations, certain copies need not be provided and corresponding information is identified in this Information Disclosure Statement by citation only. In particular,

- In accordance with 37 C.F.R. § 1.98(a)(2)(ii), copies of cited U.S. Patents and U.S. Patent Application Publications are not included.
- Certain information was submitted to, or cited by, the Office in Application No(s). N/A, filed N/A, to which the above-identified application claims priority under 35 U.S.C. § 120. In accordance with 37 C.F.R. § 1.98(d), copies of that information are not included.
- Pursuant to 1287 OG 163 (October 19, 2004), for those cited pending U.S. patent applications filed (or which entered the national stage under 35 U.S.C. § 371) on or after June 30, 2003 or which are otherwise stored in the USPTO's Image File Wrapper system, copies are not included.

FEE AUTHORIZATION

- This Information Disclosure Statement is filed within three months of the filing date of a national application other than a continued prosecution application under § 1.53(d) or within three months of entry of the national stage as set forth in § 1.491 in an international application. Therefore, no fee is required.
- The undersigned believes that this Information Disclosure Statement is being filed before the mailing date of a first Office action on the merits or before the mailing date of a first Office action after the filing of a request for continued examination under § 1.114. Therefore, no fee is believed required.

If however, this Information Disclosure Statement is filed after the period specified in § 1.97(b), the undersigned hereby authorizes the Commissioner to charge the fee set forth in § 1.17(p) to Deposit Account No. 50-0631.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

- deposited with the US Postal Service with sufficient postage as first class mail, in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
- facsimile transmitted to the US Patent and Trademark Office.



Mark Zagorin



Date
12/7/04

Respectfully submitted,



Mark Zagorin, Reg. No. 36,067

Attorney for Applicant(s)

(512) 338-6311

(512) 338-6301 (fax)

| | |
|---------------------|-------|
| EXPRESS MAIL LABEL: | _____ |
|---------------------|-------|

| | | |
|--|--|--|
| PTO/SB/08A (Substitute for form 1449/PTO) | | Attorney Docket No.: 004-9388 |
| | | Application No.: 10/626,420 |
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT | | First Named Inventor: Sheueling Chang Shantz |
| (Use several sheets if necessary) | | Filing Date: July 24, 2003 |
| | | Group Art Unit: 2131 |
| | | Examiner Name: Ayaz R. Sheikh |
| | | Date Submitted: December 7, 2004 |

U.S. PATENT DOCUMENTS

| Examiner Initials* | Cite No. ¹ | Document Number Number-Kind Code ² (if known) | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|--------------------|-----------------------|--|--------------------------------|--|---|
| | | US-5,121,431 | 06-09-1992 | Wiener | |
| | | US-6,633,896 B1 | 10-14-2003 | Moore et al. | |
| | | US- | | | |

FOREIGN PATENT DOCUMENTS

| Examiner Initials* | Cite No. ¹ | Foreign Patent Document Country Code ³ -Number ⁴ -Kind Code ⁵ (if known) | Publication Date MM-DD-YYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear | T ⁶ |
|--------------------|-----------------------|---|-------------------------------|--|---|----------------|
| | | EP 0 247 383 A3 | 12-02-1987 | Hasebe | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | | | |
|--------------------|--|-----------------|--|
| Examiner Signature | | Date Considered | |
|--------------------|--|-----------------|--|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional).

² See Kinda Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04.

³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3).

⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.

⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible.

⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14.

| PTO/SB/08B (Substitute for form 1449/PTO) | | Attorney Docket No.: 004-9388 | |
|---|-----------------------|---|----------------|
| | | Application No.: 10/626,420 | |
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use several sheets if necessary) | | First Named Inventor: Sheueling Chang Shantz | |
| | | Filing Date: July 24, 2003 | |
| | | Group Art Unit: 2131 | |
| | | Examiner Name: Ayaz R. Sheikh | |
| | | Date Submitted: December 7, 2004 | |
| NON PATENT LITERATURE DOCUMENTS | | | |
| Examiner Initial* | Cite No. ¹ | Include name of author (in CAPITAL LETTERS), title of article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T ² |
| | | Yvonne Hitchcock, et al., "Implementing an efficient elliptic curve cryptosystem over GF(p) on a smart card," ANZIAM J. 44(E), April 2003, pp. C354-C377. | |
| | | National Institute of Standards and Technology, "Recommended Elliptic Curves for Federal Government Use," August 1999, 43 pages. | |
| | | Hasegawa, Toshio, et al., "A Practical Implementation of Elliptic Curve Cryptosystems over GF(p) on a 16-bit Microcomputer," In <i>Public Key Cryptography PKC '98</i> , vol. 1431 of <i>Lecture Notes in Computer Science</i> , pages 182-194. | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Examiner Signature | | Date Considered | |

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional).

2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14.